zessen der herstellenden Unternehmen oder aus Software, die aufgrund mangelnder Rechen- und Speicherkapazität unsichere Protokolle nutzt.

Darüber hinaus stellen die herstellenden Unternehmen häufig keine Patches bereit, so dass unsichere GA-relevante Komponenten auch über einen sehr langen Zeitraum genutzt werden. Verstärkt wird die Gefährdung dadurch, dass in der GA Zugriffe auch auf solche Komponenten freigeschaltet werden müssen.

2.4. Fehlerhafte Konfiguration der Gebäudeautomation

Je nachdem, welche Bereiche der GA fehlerhaft konfiguriert sind, kann es zu Beeinträchtigungen in Betriebsabläufen, zu nicht erlaubtem physischen Zugang zu geschützten Bereichen, zu Schäden an Systemen bis hin zu Gebäude- und Personenschäden kommen.

Beispiele hierfür sind:

- Fehlerhaft konfigurierte Klimatisierung, die zu Überhitzung und Ausfall von IT-Systemen oder bei entsprechenden Wetterlagen sogar zu Beeinträchtigungen der Gesundheit von Personen führen kann.
- Nicht abgestimmt konfigurierte Systeme der Gebäudetechnik können zu Personen- und Systemschäden führen, wenn beispielsweise Strom- und Löschanlagen nicht koordiniert betrieben werden.
- Ebenso können fehlerhaft konfigurierte Zugangssysteme zu Personenschaden führen, wenn Türen im Notfall nicht geöffnet werden können.

Die Gefährdung ist für die GA besonders relevant, da aus Mangel an Testmöglichkeiten eine fehlerhafte Konfiguration vor Produktivsetzung häufig nicht erkannt werden kann. Dies kann auch bei einem fehlerhaften Update oder einem fehlerbehafteten Update-Verlauf, der ein System der GA unbrauchbar macht, auftreten.

2.5. Manipulation der Schnittstellen von eigenständigen TGA-Anlagen zur Gebäudeautomation

Manipulierte Schnittstellen zwischen GA-Systemen und gekoppelten TGA-Anlagen können in der GA zu fehlerhaften Reaktionen führen.

Ein Beispiel hierfür ist, dass eine manipulierte Meldung einer Brandmeldeanlage dazu führen kann, dass alle Türen automatisiert geöffnet werden und so unbefugten Personen Zutritt zum Gebäude gewährt wird.

2.6. Unzureichend geschützte Zugänge zur GA

Die GA umfasst eine Vielzahl von Komponenten, die anlagenübergreifende Informationen bereitstellen, austauschen und empfangen, z. B. zur Standortbestimmung von Personal oder zur Raumautomatisierung. Die Geräte kommunizieren über LAN und WLAN, aber auch über sonstige drahtlose Techniken wie beispielsweise Bluetooth.

Sind solche Netzzugänge nicht angemessen geschützt, können hierüber DoS-Angriffe durchgeführt werden. Auch können die Systeme der GA manipuliert oder sabotiert und gegebenenfalls sogar die gesamte IT der Institution erreicht werden. Manipulierte Systeme der GA können dann ein erhöhtes Datenaufkommen bis hin zu einer Überlastung der Netze und Komponenten bedingen. Auch ein Datenabfluss oder das Einspielen von Schadsoftware ist über einen unzureichend geschützten Zugang möglich.

2.7. Unzureichend abgesicherte Bedienelemente der GA

Wenn gut zugängliche Bedienelemente der GA unzureichend abgesichert sind, kann über diese die GA angegriffen werden. Beispiele hierfür sind wandmontierte Bedienelemente oder aber auch Bedienelemente von Pfortenpersonal, mit denen z. B. entfernte Türen oder Tore geöffnet werden können.

Ist der Zugang zu solchen Bedienelementen unzureichend geschützt, z. B. durch fehlende Authentisierung, kann ein unbefugter Zugriff ermöglicht werden.

Ebenfalls können unzureichend geschützte Anschlüsse von Bedienelementen, wie LAN- oder USB-Schnittstellen, einen unbefugten Zugang bieten.

2.8. Unzureichend abgesicherte Mobilfunk-Anschlüsse

Häufig müssen insbesondere in der Feld- und Automatisierungsebene GA-Komponenten genutzt werden, die über eine Mobilfunkschnittstelle mit dem jeweiligen herstellenden Unternehmen oder mit Dienstleistenden wie etwa einem Wetterdienst verbunden sind. Sind diese Schnittstellen und die Kommunikation unzureichend geschützt und dauerhaft aktiv, bieten sie Unbefugten oder bei Angriffen einen Zugriff auf das GA-Netz.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.14 *Gebäudeautomation* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Haustechnik
Weitere Zuständigkeiten	Planende, IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.14.A1 Planung der Gebäudeautomation (B) [Planende]

Für die von der Gebäudeautomation (GA) gesteuerten Gewerke MUSS festgelegt werden, wie die GA sicher gestaltet werden kann.

Die GA MUSS bereits bei der Planung von Neubau, Umbau, Erweiterung und Sanierung eines Gebäudes berücksichtigt werden. Daher MUSS die GA in den Planungs- und Bauprozessen, auch in Verbindung mit Building Information Modeling (BIM), für alle GA-relevanten Komponenten und TGA-Anlagen berücksichtigt werden.

Im Rahmen der GA-Planung MÜSSEN die einzurichtenden GA-Systeme spezifiziert werden. Es MUSS festgelegt werden, in welchem Umfang TGA-Anlagen über das GA-System automatisiert gesteuert werden sollen.

Die GA SOLLTE so geplant werden, dass zur Kopplung und Integration der TGA-Anlagen möglichst wenig unterschiedliche GA-Systeme sowie Kommunikationsprotokolle und -schnittstellen genutzt werden. Es SOLLTEN sichere und standardisierte Protokolle und Schnittstellen eingesetzt werden. Für eine Entscheidung hinsichtlich der notwendigen Systeme, Protokolle und Schnittstellen SOLLTE die erwartete Funktionalität gegenüber einem gegebenenfalls erhöhten Aufwand für Betriebs- und Informationssicherheit abgewogen werden.

Die Planung SOLLTE dokumentiert, regelmäßig und zusätzlich bei Bedarf aktualisiert und dem Stand der Technik angepasst werden.

Darüber hinaus SOLLTE die Planung regelmäßig und zusätzlich bei Bedarf mit der aktuellen Konfiguration verglichen werden (Soll-Ist-Vergleich).

INF.14.A2 Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA (B)

Aufgrund der Vielzahl von TGA-Anlagen und Komponenten in Gebäuden, die in GA-Systemen angebunden werden, MUSS der Ablauf zur Inbetriebnahme der involvierten TGA-Anlagen und GA-relevanten Komponenten aufeinander abgestimmt und übergreifend festgelegt werden. Dieser Ablauf MUSS koordiniert umgesetzt werden, um ein voll funktionsfähiges Gebäude zu gewährleisten.

Ebenso MÜSSEN klare Schnittstellen zwischen den betreibenden Organisationen der GA und der GA-relevanten Komponenten sowie den betreibenden Organisationen der TGA-Anlagen definiert werden.

Inbetriebnahme- und Schnittstellenmanagement MÜSSEN dokumentiert werden. Sowohl regelmäßig als auch zusätzlich bei Bedarf MÜSSEN die Festlegungen geprüft und gegebenenfalls nachjustiert werden. Insbesondere bei Änderungen innerhalb der GA-Systeme MÜSSEN die Festlegungen angepasst werden.

INF.14.A3 Sichere Anbindung von TGA-Anlagen und GA-Systemen (B)

Für alle TGA-Anlagen, GA-Systeme und GA-relevanten Komponenten MUSS festgelegt werden, ob durch andere TGA-Anlagen, GA-Systeme oder GA-relevante Komponenten Aktionen ausgelöst werden dürfen. Falls eine solche Integration zulässig ist, SOLLTE reglementiert werden, welche automatisierten Aktionen durch welche Informationen eines GA-Systems ausgelöst werden dürfen.

Falls eine TGA-Anlage nicht in ein GA-System integriert werden kann oder darf, diese jedoch an ein GA-System gekoppelt werden soll, MUSS festgelegt werden, welche Informationen der TGA-Anlage an das GA-System gemeldet werden.

Sowohl die Integration von TGA-Anlagen in ein GA-System als auch die rückwirkungsfreie Kopplung von TGA-Anlagen an GA-Systeme MÜSSEN angemessen abgesichert sein. Ebenfalls MUSS die Anbindung von GA-Systemen untereinander angemessen abgesichert werden.

Hierzu MÜSSEN insbesondere die Ablauf- und Funktionsketten innerhalb eines GA-Systems bzw. zwischen GA-Systemen angemessen geplant werden. Hierbei MÜSSEN alle Übergänge zwischen Gewerken und Techniken berücksichtigt werden.

Diese Ablauf- und Funktionsketten MÜSSEN umfassend getestet und bei Fehlverhalten nachjustiert werden.

Die Festlegungen MÜSSEN vollumfänglich dokumentiert werden. Sowohl regelmäßig als auch ergänzend bei Bedarf SOLLTE geprüft werden, ob die Dokumentation noch aktuell ist. Bei Abweichungen MUSS die Ursache für die Abweichungen eruiert und behoben werden.

INF.14.A4 Berücksichtigung von Gefahrenmeldeanlagen in der GA (B) [Planende]

Gefahrenmeldeanlagen inklusive Sicherheitsanlagen MÜSSEN rückwirkungsfrei an GA-Systeme gekoppelt werden. Sie DÜRFEN NICHT in ein GA-System integriert werden.

Für die netztechnische Anbindung MÜSSEN physisch getrennte Netzkomponenten und physisch getrennte Segmente genutzt werden. Werden Funknetze zur Kopplung genutzt, MÜSSEN solche TGA-Anlagen als Primärnutzende für die verwendeten Frequenzbereiche festgelegt werden. Für die Kommunikation über Funknetze SOLLTEN zertifizierte Mechanismen genutzt werden.

INF.14.A5 Dokumentation der GA (B)

Für die GA MUSS die Vielzahl unterschiedlicher Komponenten und Zugänge dokumentiert werden. Die Dokumentation MUSS regelmäßig und bei Änderungen innerhalb der GA geprüft und angepasst werden.

Insbesondere MÜSSEN auch alle deaktivierten physischen Kommunikationsschnittstellen, Protokolle und Zugänge bzw. Zugriffsmöglichkeiten zur GA dokumentiert werden. Darüber hinaus MÜSSEN alle Wechselwirkungen und Abhängigkeiten von GA-relevanten Komponenten sowie von TGA-Anlagen, die in GA-Systeme integriert oder mit GA-Systemen gekoppelt sind, dokumentiert werden. Die verfügbaren und genutzten Sicherheitseigenschaften der verwendeten Protokolle SOLLTEN dokumentiert werden.

Die Dokumentation SOLLTE für alle GA-Systeme übergreifend hinsichtlich Inhalten und deren Datenstrukturen abgestimmt werden.

INF.14.A6 Separierung von Netzen der GA (B) [Planende, IT-Betrieb]

GA-Netze MÜSSEN von Büro-Netzen und sonstigen Netzen der Institution mindestens logisch getrennt werden. Jegliche Kommunikation zwischen GA-Systemen und sonstigen IT-Systemen MUSS kontrolliert und reglementiert werden. Hierfür MÜSSEN an allen Übergängen einer solchen Segmentierung entsprechende Komponenten mit Sicherheitsfunktionen, mindestens mit Firewall-Funktion, vorgesehen werden.

Wird die GA für einen Gebäudekomplex oder eine Liegenschaft zentral eingerichtet, so MUSS die gebäudeübergreifende GA-Kommunikation über LAN-, WLAN-, WAN-, Funknetz- oder Internet-Verbindungen auch auf Ebene des Netzes separiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.14.A7 Festlegung einer Sicherheitsrichtlinie für die GA (S)

Ausgehend von der allgemeinen Sicherheitsleitlinie der Institution und der übergreifenden Sicherheitsrichtlinie für das TGM SOLLTEN die Sicherheitsanforderungen an die GA, d. h. für alle GA-Systeme, in einer GA-Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Personen, die an Planung, Beschaffung, Implementierung und Betrieb der GA-Systeme beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Inhalte und die Umsetzung der geforderten Richtlinieninhalte SOLLTEN regelmäßig überprüft, gegebenenfalls angepasst und die Ergebnisse der Prüfung nachvollziehbar dokumentiert werden.

In der Sicherheitsrichtlinie SOLLTEN auch die Vorgaben an Entwicklung und Test für den Einsatz von GA-Systemen spezifiziert werden.

INF.14.A8 Anforderungsspezifikation für GA-Systeme (S)

Ausgehend von der GA-Sicherheitsrichtlinie SOLLTE für die GA eine übergreifende und für jedes GA-System eine eigene Anforderungsspezifikation erstellt werden. Aus den Anforderungen SOLLTEN sich alle wesentlichen Elemente für Architektur und Design des jeweiligen GA-Systems und der Kopplung von GA-Systemen ableiten lassen.

Die Anforderungsspezifikation SOLLTE dokumentiert sowie regelmäßig und zusätzlich bei Bedarf dem Stand der Technik angepasst werden. Darüber hinaus SOLLTE regelmäßig die Umsetzung der Anforderungen geprüft werden.

Es SOLLTEN in der GA ausschließlich Komponenten eingesetzt werden, die eine Authentisierung mindestens über einen änderbaren Anmeldenamen und ein änderbares Passwort bereitstellen.

INF.14.A9 Entwicklung eines GA-Konzepts (S)

Ausgehend von der GA-Sicherheitsrichtlinie und den Anforderungsspezifikationen SOLLTE für die GA ein übergreifendes GA-Konzept entwickelt werden. Hieraus abgeleitet SOLLTEN für alle GA-Systeme detaillierte Konzepte entwickelt werden. In den Konzepten SOLLTEN mindestens folgende Punkte angemessen berücksichtigt werden:

- alle in das jeweilige GA-System integrierten TGA-Anlagen
- alle mit dem jeweiligen GA-System gekoppelten TGA-Anlagen
- alle GA-relevanten Komponenten mit den jeweiligen Kommunikationsverbindungen

Die Konzepte SOLLTEN alle technischen und organisatorischen Vorgaben beschreiben. Die erstellten Konzepte SOLLTEN regelmäßig geprüft und gegebenenfalls aktualisiert werden.

INF.14.A10 Bildung von unabhängigen GA-Bereichen (S) [Planende]

In der GA SOLLTEN GA-Bereiche derart geplant und umgesetzt werden, dass Abhängigkeiten zwischen den GA-Bereichen minimiert werden und GA-Bereiche unabhängig gesteuert werden können. Eine Störung in einem GA-Bereich SOLLTE keine oder nur geringe Auswirkungen auf andere GA-Bereiche haben.

Insbesondere SOLLTEN die Gebäude innerhalb eines Gebäudekomplexes oder einer Liegenschaft separat steuerbar sein.

Die eingerichteten GA-Bereiche SOLLTEN auch im GA-Managementsystem entsprechend sichtbar sein.

INF.14.A11 Absicherung von frei zugänglichen Ports und Zugängen der GA (S) [Planende]

Der Anschluss von Komponenten, speziell von unautorisierten, unbekannten Komponenten und Fremdgeräten, SOLLTE insbesondere an frei zugänglichen Ethernet-Ports, USB-Ports und anderen Schnittstellen der GA kontrolliert und eingeschränkt werden.

Der Anschluss einer unautorisierten oder unbekannten Komponente SOLLTE in die Ereignisprotokollierung aufgenommen werden. Eine direkte IP-basierte Kommunikation von solchen Komponenten mit Systemen der GA SOLLTE unterbunden werden (siehe INF.14.A13 *Netzsegementierung in der GA*).

Für frei zugängliche LAN- oder WLAN-Zugänge SOLLTE eine Netzzugangskontrolle gemäß IEEE 802.1X oder vergleichbare Sicherheitsmechanismen eingesetzt werden. Hiermit SOLLTEN unzureichend authentisierte und autorisierte Komponenten in getrennten Netzsegmenten positioniert werden.

Frei zugängliche Schnittstellen für temporäre Wartungszwecke, wie beispielsweise USB-Ports an GA-Komponenten, SOLLTEN nur bei Bedarf aktiviert werden.

INF.14.A12 Nutzung sicherer Übertragungsprotokolle für die GA (S)

Für Konfiguration, Wartung und Steuerung von GA-relevanten Komponenten, die auf Ethernet und IP basieren, SOLLTEN sichere Protokolle eingesetzt werden, falls nicht über vertrauenswürdige Netzsegmente kommuniziert wird.

Außerhalb vertrauenswürdiger Netzsegmente SOLLTE die Kommunikation über Ethernet und IP zwischen GA-Systemen verschlüsselt erfolgen. Die Verschlüsselung SOLLTE mit den jeweils aktuellen Verschlüsselungsmechanismen durchgeführt werden.

INF.14.A13 Netzsegmentierung in der GA (S) [Planende]

Innerhalb des GA-Netzes SOLLTE eine Netzsegmentierung umgesetzt werden, die bedarfsgerecht einzelne GA-Systeme, einzelne TGA-Anlagen oder einzelne Gruppen von TGA-Anlagen innerhalb eines GA-Systems voneinander trennt.

Für die Übergänge zwischen den Segmenten SOLLTEN entsprechende Regeln definiert und zur Umsetzung Komponenten mit Sicherheitsfunktionen, mindestens zustandsbehaftete Paketfilter, genutzt werden.

INF.14.A14 Nutzung eines GA-geeigneten Zugriffsschutzes (S)

Für die GA SOLLTE ein Identitäts- und Berechtigungsmanagement gemäß Baustein ORP.4 *Identitäts und Berechtigungsmanagement* genutzt werden, das die Anforderungen der GA angemessen umsetzt. Hierfür SOLLTE bedarfsabhängig eine GA-eigene Authentisierungslösung oder eine geeignete Replikation einer zentralen Authentisierungslösung der Institution realisiert werden. In die Authentisierungslösung SOLLTEN soweit möglich alle GA-relevanten Komponenten eingebunden werden.

Betreibende der GA-Systeme, Betreibende der TGA-Anlagen und auch Nachfrageorganisationen SOLLTEN im Rollen- und Berechtigungskonzept hinsichtlich der GA angemessen berücksichtigt werden. Dies SOLLTE insbesondere dann sorgfältig geplant und abgestimmt werden, wenn die GA institutionsübergreifend bereitgestellt wird.

Alle GA-relevanten Komponenten, inklusive der Komponenten der Feldebene und Bedienelemente, SOLLTEN geeignete Funktionen zur Absicherung von Zugriffen umsetzen können. Komponenten, die keinen Zugriffsschutz bieten oder für die vom herstellenden Unternehmen vorgegebenen Zugangsparameter nicht änderbar sind, SOLLTEN NICHT genutzt werden.

INF.14.A15 Absicherung von GA-spezifischen Netzen (S)

Sind in GA-spezifischen Netzen wie z. B. BACnet Sicherheitsmechanismen der Kommunikation verfügbar, SOLLTEN diese genutzt werden. Mindestens SOLLTEN Mechanismen zur Authentisierung und Verschlüsselung genutzt werden.

Für GA-spezifische Netze, die keine angemessenen Sicherheitsmechanismen realisieren können, SOLLTE erwogen werden, diese auf ein GA-spezifisches Netz mit angemessenen Sicherheitsmechanismen umzustellen.

Grundsätzlich SOLLTE die Kommunikation mit GA-spezifischen Netzen durch Koppelelemente mit Sicherheitsfunktionen kontrolliert und gegebenenfalls reglementiert werden.

INF.14.A16 Absicherung von drahtloser Kommunikation in GA-Netzen (S) [Planende]

In GA-Netzen, die auf einer drahtlosen Kommunikation wie z. B. EnOcean basieren, SOLLTEN die Sicherheitsmechanismen der jeweiligen Funktechnik zur Absicherung der Kommunikation genutzt werden. Insbesondere SOLLTEN eine angemessene Authentisierung und eine Verschlüsselung auf der Luftschnittstelle umgesetzt werden. Ist dies

für die entsprechenden Endgeräte nicht möglich, SOLLTE für diese Endgeräte die Kommunikation am Übergang in kabelgebundene Netze kontrolliert werden, z. B. durch eine Komponente mit Firewall-Funktion.

Darüber hinaus SOLLTEN mögliche Störungen für die Ausbreitung der Funkwellen, beispielsweise durch Abschattungen, bei der Planung der GA-Netze berücksichtigt werden.

INF.14.A17 Absicherung von Mobilfunkkommunikation in GA-Netzen (S) [Planende]

Wird im Rahmen der GA Mobilfunk eingesetzt, SOLLTEN für solche GA-Netze die Sicherheitsmechanismen der jeweiligen Mobilfunknetze genutzt werden.

Werden öffentliche Mobilfunknetze wie 5G oder Sigfox in der GA verwendet, SOLLTE eine unkontrollierte direkte IP-basierte Kommunikation mit GA-relevanten Komponenten unterbunden werden.

GA-Komponenten SOLLTEN nur dann mit einem dedizierten Anschluss an ein öffentliches Mobilfunknetz ausgestattet werden, falls dieser für deren Betrieb essenziell ist. Hierfür SOLLTE geprüft und festgelegt werden, für welche GA-Komponenten ein Anschluss an öffentliche Mobilfunknetze notwendig ist.

Sofern im öffentlichen Mobilfunknetz keine Trennung der GA-Netze möglich ist, wie z. B. bei 5G mit Slicing, SOLLTE im Kommunikationspfad eine Entkopplung der IP-Kommunikation durch ein Application Layer Gateway (ALG) stattfinden.

Falls Mobilfunktechniken in der GA als Bestandteil der öffentlichen Mobilfunkinfrastruktur eines Mobilfunkunternehmens eingesetzt werden, SOLLTEN mit den Mitteln der entsprechenden Mobilfunktechnik ein oder mehrere virtuelle Mobilfunknetze realisiert werden, die ausschließlich der GA zur Verfügung stehen.

Falls in der GA mit Hilfe von Mobilfunktechniken wie LTE und 5G autarke private Mobilfunknetze lokal auf dem Campus eingerichtet werden, SOLLTE der Übergang zwischen diesen Mobilfunknetzen und den sonstigen Netzen durch ein Koppelelement mit Firewall-Funktion abgesichert werden. Auch für private Mobilfunknetze SOLLTE eine Segmentierung in mehrere virtuelle Mobilfunknetze umgesetzt werden.

INF.14.A18 Sichere Anbindung von GA-externen Systemen (S)

Die Kommunikation von GA-Systemen mit GA-externen Systemen SOLLTE ausschließlich über definierte Schnittstellen und mit definierten IT-Systemen möglich sein. Die Kommunikation SOLLTE authentisiert und verschlüsselt werden.

Die möglichen Schnittstellen zu GA-externen Systemen SOLLTEN auf das notwendige Maß beschränkt werden.

INF.14.A19 Nutzung dedizierter Adressbereiche für GA-Netze (S) [Planende]

Für die GA SOLLTEN dedizierte Adressbereiche genutzt werden, die sich insbesondere von den Adressbereichen der Büro-IT und der OT unterscheiden. Für diese Adressbereiche SOLLTE festgelegt werden, aus welchen Bereichen statische Adressen vergeben werden und welche GA-relevanten Komponenten statische Adressen erhalten.

Falls an die GA angebundene Netzbereiche wie TGA-Anlagen identische Adressbereiche nutzen (Replizieren von Anlagenkonfigurationen), MÜSSEN diese in getrennten Segmenten positioniert werden, um Adresskonflikte zu unterbinden. In diesem Fall MUSS die segmentübergreifende Kommunikation durch entsprechende Mechanismen abgesichert werden, beispielsweise durch den Einsatz eines ALG oder von Network Address Translation (NAT).

INF.14.A20 Vermeidung von Broadcast-Kommunikation in GA-Netzen (S) [Planende]

In GA-Netzen SOLLTE die Broadcast-Last auf OSI Layer 2 oder OSI Layer 3 für unbeteiligte Systeme und Komponenten minimiert werden, um eine Überlastung zu vermeiden. Hierzu SOLLTE die Kommunikation auf gruppenspezifische Multicasts umgestellt oder in der Planung der Segmentierung entsprechend berücksichtigt werden.

INF.14.A21 Anzeigen der Gültigkeit von Informationen in GA-Systemen (S)

Ein GA-System SOLLTE visualisieren, ob die angezeigten Informationen bezüglich Zeit, Ort, Wert, Zustand oder Ereignis auf planmäßig erhaltenen Informationen basieren. Informationen, die simulierte oder „eingefrorene" Werte anzeigen, SOLLTEN abhängig vom Schutzbedarf der TGA-Anlagen erkennbar sein oder einen Alarm auslösen.

INF.14.A22 Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen (S) [Planende]

Innerhalb eines GA-Systems SOLLTE sichergestellt werden, dass TGA-Anlagen gemäß ihrem Schutzbedarf auch unabhängig von der Anbindung an das GA-System autark funktionieren. Insbesondere SOLLTEN GA-Systeme so konfiguriert werden, dass keine betriebsverhindernden Abhängigkeiten zum TGM, zu anderen GA-Systemen oder TGA-Anlagen bestehen. Eine TGA-Anlage SOLLTE auch bei Ausfall der Verbindung zur GA für einen bestimmten Zeitraum gemäß dem jeweiligen Schutzbedarf betriebsfähig bleiben und ihre Funktion wahrnehmen.

INF.14.A23 Einsatz von physisch robusten Komponenten für die GA (S) [Planende]

Abhängig von den Einsatzbedingungen der Komponenten in der GA SOLLTEN entsprechend physisch robuste Komponenten eingesetzt werden, die besonders auch für harsche Umgebungsbedingungen vorgesehen bzw. ausgewiesen sind. Sind angemessen robuste Komponenten nicht verfügbar, SOLLTEN entsprechende Kompensationsmaßnahmen ergriffen werden.

INF.14.A24 Zeitsynchronisation für die GA (S)

Alle in einem GA-System angebundenen Komponenten und TGA-Anlagen SOLLTEN eine synchrone Uhrzeit nutzen, um ein automatisiertes Messen, Steuern und Regeln zu gewährleisten (siehe auch Baustein OPS.1.2.6 *NTP-Zeitsynchronisation*). Auch GA-Systeme, die miteinander verbunden sind, SOLLTEN eine synchrone Uhrzeit nutzen. Erstreckt sich die GA über Gebäudekomplexe oder Liegenschaften, SOLLTE die Zeitsynchronisation für alle Gebäude gewährleistet werden.

Falls innerhalb eines GA-Systems eine Kommunikation mit Echtzeit-Anforderungen erforderlich ist, SOLLTE für die Zeitsynchronisation PTP oder ein vergleichbarer Mechanismus anstelle von NTP genutzt werden.

INF.14.A25 Dediziertes Monitoring in der GA (S)

Für alle Komponenten, die für die GA betriebsrelevant sind, SOLLTE ein geeignetes Monitoringkonzept erstellt und umgesetzt werden. Hierbei SOLLTEN die Verfügbarkeit sowie bedeutsame Parameter der GA-relevanten Komponenten laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN automatisch an die betreibende Organisation gemeldet werden.

Es SOLLTEN durch die GA mindestens Alarme ausgelöst werden, wenn TGA-Anlagen ausfallen oder wichtige Funktionen zum automatisierten Steuern und Regeln nicht verfügbar sind. Zudem SOLLTE festgelegt werden, für welche besonders sicherheitsrelevanten Ereignisse und für welche weiteren Ereignisse automatische Alarmmeldungen generiert werden.

Statusmeldungen und Monitoringdaten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

INF.14.A26 Protokollierung in der GA (S)

Ergänzend zum Baustein OPS.1.1.5 *Protokollierung* SOLLTEN Statusänderungen an GA-relevanten Komponenten und sicherheitsrelevante Ereignisse protokolliert werden. Zusätzlich SOLLTEN alle schreibenden Konfigurationszugriffe auf TGA-Anlagen und gegebenenfalls GA-relevante Komponenten sowie alle manuellen und automatisierten Änderungen der Zustände von diesen protokolliert werden.

Es SOLLTE festgelegt werden, welche Protokollierungsdaten auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

INF.14.A27 Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung (S)

Es SOLLTE initial und in regelmäßigen Abständen nachvollziehbar analysiert werden, wie sich die GA und die abgeleiteten Planungen und Konzepte auf die Notfallplanung auswirken. Insbesondere SOLLTE festgelegt werden, wie bei einem Ausfall von TGA-Anlagen oder GA-relevanten Komponenten durch technischen Defekt oder Angriff die Wechselwirkungen auf andere TGA-Anlagen, GA-relevante Systeme und TGM minimiert werden können. Im Rahmen der Notfallplanung SOLLTE auch festgelegt werden, welches Wartungspersonal für die betroffenen TGA-Anlagen und GA-relevanten Systeme zuständig ist und über welche Meldewege dieses erreicht werden kann. Außerdem SOLLTE festgelegt werden, welche Berechtigungen das Wartungspersonal zur Behebung von Notfällen hat.

Es SOLLTE in der Notfallplanung auch spezifiziert werden, wie bei Ausfall der GA-Systeme ein gegebenenfalls erforderlicher Notbetrieb von TGA-Anlagen sichergestellt wird. Dabei SOLLTE für alle TGA-Anlagen und GA-Systeme inklusive aller GA-relevanten Komponenten eine Wiederanlaufreihenfolge festgelegt und in den entsprechenden Wiederanlaufplänen dokumentiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.14.A28 Physische Trennung der GA (H) [Planende]

Bei erhöhtem Schutzbedarf SOLLTEN GA-Netze als physisch getrennte Zonen gemäß Baustein NET.1.1 *Netzarchitektur und -design* realisiert werden.

Abhängig vom Schutzbedarf SOLLTE für die Anbindung beispielsweise an externe Clouds ein dedizierter, restriktiv reglementierter Internet-Zugang bereitgestellt werden.

Ebenfalls SOLLTEN, abhängig vom Schutzbedarf der GA-Systeme, Anbindungen an nicht vertrauenswürdige Netze, gegebenenfalls auch Anbindungen an institutionseigene Büro- oder OT-Netze, unterbunden werden.

INF.14.A29 Trennung einzelner TGA-Anlagen (H)

Um einzelne TGA-Anlagen mit erhöhtem Schutzbedarf innerhalb eines GA-Systems abzusichern, SOLLTEN solche TGA-Anlagen in separaten Netzsegmenten positioniert werden. Zur Kontrolle der Kommunikation SOLLTEN Firewall-Funktionen unmittelbar vor dem Anlagennetz positioniert werden.

INF.14.A30 Bereitstellung eines GA-eigenen Zeitservers zur Zeitsynchronisation (H)

Bei erhöhtem Schutzbedarf SOLLTE für die GA oder auch für einzelne GA-Systeme ein eigener GA-Zeitserver bereitgestellt werden, der direkt mit einer Atom- oder Funkuhr (Stratum 0) gekoppelt ist und an den gegebenenfalls weitere nachgelagerte GA-Zeitserver angebunden werden.

4. Weiterführende Informationen

4.1. Genutzte GA-spezifische Fachbegriffe

Anlagenautomation (englisch System Automation and Control, SAC)

Die Anlagenautomation (AA) ist ein Teil eines GA-Systems und realisiert die Automation zum energieeffizienten, wirtschaftlichen und sicheren Betrieb von Anlagen der TGA. Die Anlagenautomation steuert über Aktoren die TGA-Anlage und dessen Zustandsgrößen. Diese werden wiederum durch die Sensoren der TGA-Anlage erfasst.

Bedien- und Beobachtungseinheiten (englisch Control and Display Device, CDD)

Gemäß DIN EN ISO 16484-2 umfasst der Begriff Bedien- und Beobachtungseinheiten (auch Leitstand oder Leitwarte genannt) die Summe der Einrichtungen für die Benutzenden, die als Schnittstelle zu den Bedien- und Managementfunktionen eines GA-Systems fungiert.

GA-Bereich (englisch BACS Area)

Ein GA-Bereich umfasst einen oder mehrere Räume ähnlicher Nutzung, die horizontal, vertikal oder gemischt verteilt sein können und mehrere GA-Segmente umfasst.

Beispiele: ein Flur, eine Etage, ein Gebäudeflügel, eine Produktionshalle.

GA-Management (englisch Management Building Automation and Control Systems, M-BACS)

Das GA-Management (GA-M), auch als Gebäudeleittechnik bezeichnet, übernimmt als Bestandteil eines GA-Systems Aufgaben zur Informationsverarbeitung für das Management der GA, beispielhaft Funktionen für ein übergeordnetes Energiemanagement, Wartungsmanagement, Störmanagement aber auch Raumbuchungsmanagement.

GA-Segment (englisch BACS Segment)

Ein GA-Segment bezeichnet die kleinste betrachtete räumliche Einheit, für die GA-Funktionen anwendbar sind. Ein GA-Segment ist nicht zu verwechseln mit einem Netzsegment, das über Sicherheitselemente vom restlichen Netz separiert wird.

GA-spezifische Netze (englisch BACS-specific Networks)

Ein GA-spezifisches Netz beschreibt ein Netz, das eine Verkabelung nutzt, die meist nicht auf Ethernet-Techniken basiert, z. B. KNX-Bussystem, oder das spezifische Protokolle nutzt, die nicht auf IP und Ethernet gemäß IEEE 802.3 basiert, z. B. BACnet. Spezifische Protokolle können aufgrund von Anforderungen an eine Echtzeitkommunikation oder an einen reduzierten Protokollumfang erforderlich werden.

GA-System (englisch Building Automation and Control System, BACS)

Ein GA-System stellt gemäß VDI 3814-1 die technische Realisierung der GA dar und umfasst die folgenden Teile:

- GA-Management
- Anlagenautomation
- Raumautomation

Anlagenautomation und Raumautomation bestehen analog zur Operational Technology (OT) aus den (funktionalen) Ebenen Automationsebene (z. B. Anlagensteuerungen) und Feldebene (z. B. Aktoren und Sensoren).

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten automatisierten Betrieb der Technischen Gebäudeausrüstung (TGA).

Gefahrenmeldeanlage (englisch Alarm System)

Gefahrenmeldeanlagen (GMA) sind TGA-Anlagen, die Gefahren wie Einbruch, Feuer und Rauch erkennen und melden können. Sie erfassen Gefahren durch Interaktion mit Sensoren oder Bedieneinheiten und erzeugen Gefahrenmeldungen, die an eine zentrale Komponente gesendet werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Integration von Systemen oder Anlagen

Eine Integration von Systemen oder Anlagen bedeutet gemäß VDI 3814, dass integrierte Systeme oder Anlagen Informationen mit dem GA-Management austauschen und sich hierdurch gegenseitig beeinflussen können.

Eine Systemintegration im Rahmen der GA ist abzugrenzen von eingebetteten Systemen (englisch Embedded Systems). Diese sind intelligente Elemente, die in andere Systeme eingebettet sind und weitestgehend unsichtbar Überwachungs-, Steuerungs-, Verarbeitungs- oder Regelfunktionen innerhalb des einbindenden Systems übernehmen.

Kopplung von Systemen oder Anlagen

Eine Kopplung von Systemen und Anlagen bedeutet gemäß VDI 3814-2-2, dass die gekoppelten Systeme (Brandmeldeanlage oder Einbruchsmeldeanlage) ihre Informationen zur GA schicken, ohne dadurch ihre Autarkie einzuschränken oder zu verlieren. Eine System- oder Anlagenkopplung ist somit grundsätzlich rückwirkungsfrei.

Beispiele: Brandmeldeanlage oder Einbruchsmeldeanlage.

Leitstand (englisch Control Center)

Ein Leitstand (siehe auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von GA-Prozessen.

Liegenschaft (englisch Property)

Eine Liegenschaft umfasst gemäß VDI 3814-1 ein oder mehrere, meist lokal benachbarte Gebäude.

Lokale Vorrangbedienung (englisch Local Override, LOR)

Eine lokale Vorrangbedienung (LVB, früher auch Notbedieneinrichtung genannt) stellt gemäß VDI 3814-1 die Schnittstelle zu GA-relevanten Komponenten, die ein eingeschränktes Betreiben unabhängig von Automationseinrichtungen mit vorrangigem Anzeigen, Schalten und/oder Stellen ermöglicht. Ein Beispiel ist der manuelle vorrangige Betrieb von Ventilatoren.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mietparteien innerhalb eines Gebäudes, Eigentümerinnen und Eigentümer eines Gebäudes, Dienstleistende innerhalb einer Institution, z. B. Kantine

Raumautomation (englisch Room Automation and Controls, RAC)

Die Raumautomation (RA) ist Bestandteil eines GA-Systems und realisiert alle Aufgaben einer anlagenübergreifenden Automation im betrachteten Raum, z. B. die Bedienung der im Raum installierten Technik.

Rückwirkungsfreiheit

Eine rückwirkungsfreie Anbindung einer TGA-Anlage an die GA bedeutet, dass die TGA-Anlage zwar Informationen an die GA liefert, von dieser jedoch auf Basis dieser Informationen nicht beeinflusst werden kann. Die Anlage bleibt weiterhin autark.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Gebäude eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der GA sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen" sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen. Anlagen werden in der GA in ein GA-System integriert oder mit GA-Systemen gekoppelt.

4.2. Abkürzungen

Abkürzung	Bedeutung
5G	5. Generation des Mobilfunks
AA	Anlagenautomation
ALG	Application Layer Gateway
BACS	Building Automation and Control Systems
BIM	Building Information Modelling
DIN	Deutsches Institut für Normung
DoS	Denial of Service

Abkürzung	Bedeutung
EN	Europäische Norm
GA	Gebäudeautomation
GMA	Gefahrenmeldeanlagen
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	Internationale Organisation für Normung
KNX	Konnex(-Bus)
LAN	Local Area Network
LTE	Long Term Evolution
MSR	Messen, Steuern, Regeln
NAT	Network Address Translation
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OT	Operational Technology
PTP	Precision Time Protocol
RA	Raumautomation
SLA	Service Level Agreement
TGA	Technische Gebäude-Ausstattung
TGM	Technisches Gebäude-Management
VDI	Verein Deutscher Ingenieure e.V.
VDMA	Verband Deutscher Maschinen- und Anlagenbau
WAN	Wide Area Network
WLAN	Wireless Local Area Network

4.3. Wissenswertes

Genannten Normen und Dokumente:

DIN EN ISO 16484 – Systeme der Gebäudeautomation (GA)

- DIN EN ISO 16484-1 – Systeme der Gebäudeautomation (GA), Teil 1: Projektplanung und -ausführung, DIN/EN/ISO, März 2011, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-2 – Systeme der Gebäudeautomation (GA), Teil 2: Hardware, DIN/EN/ISO, Oktober 2004, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-3 – Systeme der Gebäudeautomation (GA), Teil 3: Funktionen, DIN/EN/ISO, Dezember 2005, verfügbar im Beuth-Verlag
- DIN EN ISO 16484-5 – Systeme der Gebäudeautomation (GA), Teil 5: Datenkommunikationsprotokoll (BACnet), DIN/EN/ISO, Dezember 2017, verfügbar im Beuth-Verlag

DIN 32736 – Gebäudemanagement – Begriffe und Leistungen, Deutsches Institut für Normung, August 2000, verfügbar im Beuth-Verlag

DIN EN ISO 41011 – Facility Management – Begriffe, DIN/EN/ISO, April 2019, verfügbar im Beuth-Verlag

DIN 276 – Kosten im Bauwesen, Deutsches Institut für Normung e.V., Dezember 2018, verfügbar im Beuth-Verlag

VDI 4700 Blatt 1 – Begriffe der Bau- und Gebäudetechnik, Verein Deutscher Ingenieure e.V., Oktober 2015, verfügbar im Beuth-Verlag

VDI 3814 – Gebäudeautomation (GA)

- VDI 3814 Blatt 1 – Gebäudeautomation (GA) – Grundlagen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 2.1 – Gebäudeautomation (GA) – Planung – Bedarfsplanung, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 2.2 – Gebäudeautomation (GA) – Planung – Planungsinhalte, Systemintegration und Schnittstellen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 2.3 – Gebäudeautomation (GA) – Planung – Bedienkonzept und Benutzeroberflächen, Verein Deutscher Ingenieure e.V., September 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 3.1 – Gebäudeautomation (GA) – Planung – GA-Funktionen – Automationsfunktionen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.1 – Gebäudeautomation (GA) – Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe – Kennzeichnung, Adressierung und Listen, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.2 – Gebäudeautomation (GA) – Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe – Bedarfsplanung, Planungsinhalte und Systemintegration, Verein Deutscher Ingenieure e.V., Januar 2019, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 4.3 – Gebäudeautomation (GA) – Methoden und Arbeitsmittel für Planung, Ausführung und Übergabe – GA-Automationsschema, GA-Funktionsliste, GA-Funktionsbeschreibung, Verein Deutscher Ingenieure e.V., November 2020, Entwurf, verfügbar im Beuth-Verlag
- VDI 3814 Blatt 6 – Gebäudeautomation (GA) – Qualifizierung, Rollen und Kompetenzen, Verein Deutscher Ingenieure e.V., April 2020, Entwurf, verfügbar im Beuth-Verlag

VDMA 24774 – IT-Sicherheit in der Gebäudeautomation, VDMA e. V., Februar 2021, verfügbar im Beuth-Verlag